Társadalom – technológiai környezet – nemzetbiztonság

Dobák Imre

A „nemzetbiztonság” működésének közege

Napjainkban a nemzetbiztonsági szolgálatok egy rendkívül összetett, dinamikusan változó világban látják el feladataikat. Működésüket számos külső tényező befolyásolja, amelyek az alábbi irányokból érkezhetnek:[1]

- a *társadalom irányából* (például érdekek módosulása, elvárások változása);
- az *állam irányából* (például állami berendezkedés, politikai rendszer, szabályozás változása);
- a *gazdaság irányából* (például erőforrások rendelkezésre állása, költségvetés kérdései);
- a *biztonságpolitika irányából* (például együttműködések, rendkívüli események bekövetkezése, biztonsági veszélyek jellemzőinek változása – például új terroristamódszerek, migráció tömeges jellege);
- valamint a fejlődő technológiai környezet irányából.

Értelemszerűen e tényezők teljességgel nem választhatók el egymástól, amelyek összetettségére a „társadalom”, a „gazdasági szereplők”, és a „nemzetbiztonsági” szféra háromszöge mentén felállítható alábbi modellel kívánunk rávilágítani. Segítségével reményeink szerint áttekinthetőbbé válnak az egymásra gyakorolt hatások, illetve az ott megjelenő, gyakran ütköző érdekek. Ebben a háromszögben:

- A *társadalom* tagjainak alapvető érdeke, hogy szabadon, határoktól és egyéb korlátoktól függetlenül kommunikáljanak, személyes adataikat szabadon védjék (akár titkosítási megoldásokat használjanak), és magánszférájukat az állam tiszteletben tartsa. A gazdasági szereplők felé ugyanakkor az egyének széles körben önként adnak felhatalmazást adataik „gyűjtésére-tárolására”, hiszen ezen adatokkal személyre

[1] Dobák Imre: Technológiai fejlődés – titkosszolgálatok. In Fekete Károly (szerk.): *Kommunikáció.* Budapest, Nemzeti Közszolgálati Egyetem, 2013. 66.

https://doi.org/10.36250/00904_04

szabottabb szolgáltatásokat kapnak, életüket megkönnyítő megoldásokhoz juthatnak. Társadalmi elvárásként jelenik meg részükről, hogy az erre a célra létrehozott biztonsági és nemzetbiztonsági szervek (nemzetbiztonság) biztonságukat garantálják.

– A *gazdasági szereplők* kategóriájához jelen modell főként az infokommunikációs és online kereskedelmi tevékenységek területén globális piacokat szerző és lényegében jelentős gazdasági és egyben politikai szereplőkké váló nagyvállalati szereplőket sorolja (például Apple, Microsoft, Google, Facebook vagy akár az Amazon). E nagyvállalatok érdekei között (legyenek azok akár nemzeti, akár globális szintű szereplők) jelennek meg, hogy a társadalom tagjainak igényeit kiszolgálva üzleti alapon biztosítsák az információs technológiákhoz és a kommunikációhoz való hozzáférés lehetőségét. Mindez sajátos viszonyrendszert eredményez a nemzetbiztonsági struktúrák irányába is, hiszen a nemzetbiztonsággal való túlzott együttműködésük felboríthatja a társadalom irányába meglévő, termékeik, szolgáltatásaik szempontjából fontos bizalmi viszonyt (és úgynevezett bizalmi deficit alakulhat ki).[2] A globális infokommunikációs szereplők esetében további jellemzőként merül fel, hogy rendkívüli, akár adott országok politikai folyamataira hatást gyakorló technológiai képességekkel rendelkeznek.
– A *nemzetbiztonsági* szféra ebben a köztes viszonyrendszerben látja el feladatát, ahol a működése mentén a társadalom érdekében végzett összetett nemzetbiztonsági feladatokat, a nemzetbiztonsági érdekek érvényesítését és közvetve az állampolgárok védelmét kell keresni. Ugyanakkor a korábbi hidegháborús viszonyokkal szemben a veszélyeket gyakran már nem egy jól látható másik fél, hanem a társadalom tagjai között meghúzódó nem békés célú egyének (bűnözők, terroristák, hackerek) is jelenthetik, akik tevékenységének felderítése sajátos (egyes esetekben a magánszféra sérülését okozó) eszközöket igényelhet. A gazdasági szereplők egyrészről együttműködési szükségletet (például hírközlési adatok beszerzése egy hírközlési szolgáltatótól), másrészről együttműködési lehetőségeket (például fejlesztések) jelentenek. Az együttműködés tartalmát és formáit a nemzetbiztonsági tevékenység érzékenysége miatt

[2] Példaként az Apple vagy akár a BlackBerry mobiltelefonok említhetők, amelyekről elterjedt, hogy nagyobb biztonságot jelenthetnek felhasználóik számára, így a vállalatok széles együttműködése a nemzetbiztonsági szférával minden bizonnyal csökkentené a termékeik iránti keresletet.

ugyanakkor a nemzetbiztonsági szféra is sajátos fenntartással kezeli. Számos ország esetében látható például a biztonsági magánvállalati szereplők fokozott szerepvállalása, de itt említhető akár egy külföldi kommunikációs szolgáltató állami kommunikáció biztosításába történő bevonásának vitatott kérdése is. Az együttműködéstől való teljes elzárkózás esetén a nemzetbiztonsági szolgálatok eszközrendszerei, megoldásai „elavulhatnak", és előtérbe kerülhet az úgynevezett *„going dark"* jelensége,[3] amely (a fejlett titkosítások szabad használata és elterjedése kapcsán jelent meg, és) egyfajta „képességvesztést" jelez a technológiailag fejlettebb környezettel szemben. A demokratikus államok nemzetbiztonsági rendszerei oldaláról így egy, az állam, a társadalom és tagjainak védelme érdekében működő olyan rendszer működtetése a cél, amely az egyének magánszférájának a lehető legkisebb sérülését okozza, ugyanakkor a külső környezet kihívásaira reagálva, a hírszerzés és a nemzetbiztonság egyéb területei szempontjából a legnagyobb hatékonyságot biztosíthatja. Ezt a hatékonyságot a képességeik és az ezek működésének kereteit biztosító jogszabályi környezet hangolásával igyekeznek elérni.

A viszonyrendszer működése

Az infokommunikáció 21. századi globális szereplői sajátos helyzetük, kutatási és termelési erőforrásaik révén szinte szabadon formálhatják a technológiai trendeket. Közös jellemzőjük, hogy túlnyomó többségük olyan technikai profilú vállalat, amely egy korábban nem létező piaci szegmensben jött létre az elmúlt 20 év során. Igazi erőforrásaik és jelentőségük magukban a „szolgáltatásaik" használatában, és a nagy mennyiségű adatok „kezelésében" rejlik. Ilyenek például az internetes keresők vagy akár a közösségi oldalak, ahol az információk kezelése, hozzáférések biztosítása a működés lényegét alkotják. Szolgáltatásaik lényegében kikerülik az adott állami szereplőket, aminek eredményeként e globális nagy nemzetközi cégek tevékenysége – az általuk szolgáltatott, a társadalom életét pozitívan támogató tagadhatatlan megoldások és fejlesztések mellett – akár az egyes államokra is közvetlen hatással lehetnek. A „digitális kapitalizmus" profitorientált nagyvállalataival szemben természetesen sajátos

[3] Peter Swire – Kenesa Ahmad: Encryption and Globalization. *The Columbia Science & Technology Law Review,* 23. (2012), Spring 464.

válaszok születnek, amelyek mentén a *szabályozás* és használat, valamint a *tiltás* folyamatos váltakozásait figyelhetjük meg.

Szabályozás

Idesorolhatók az Európai Unió szintjén megjelenő, globális szolgáltatókkal szembeni büntetések és a monopolhelyzettel kapcsolatos vizsgálatok. Ki kell emelni az állampolgárok személyi adatai fokozottabb védelmének területét, amelyre jó példa az EU általános adatvédelmi rendeletének (GDPR)[4] 2018 óta történő kötelező alkalmazása,[5] valamint az állampolgárok személyes adatainak EU-n kívüli fél részére történő átadási kereteinek újraszabályozása. Az Európai Unióból az Amerikai Egyesült Államok felé – adott feltételek megléte esetén – történő személyes adatok továbbítására az Európai Bizottság 2000-ben elfogadott határozata (Biztonságos Kikötő Adatvédelmi Alapelvek – úgynevezett „Safe Harbor Privacy Principles") adott lehetőséget, amelyet az Európai Bíróság 2015-ben érvénytelenített,[6] majd 2016-ban már amerikai kormánygaranciákkal új megállapodást (EU–USA Adatvédelmi Pajzs – *Privacy Shield*) hoztak létre.[7] Az infokommunikációs megoldásokhoz köthető adatvédelmi igények a nagy globális infokommunikációs szolgáltatóktól is számos lépés megtételét követelték. Előtérbe került a felhasználók megfelelő tájékoztatásának követelménye az adataik felhasználásáról, kezeléséről és őrzéséről.

[4] General Data Protection Regulation – 2016-ban hatályba lépett, 2018-tól alkalmazott európai szintű általános adatvédelmi rendelet a természetes személyek személyes adatainak kezeléséről, védelméről.

[5] Az Európai Unióban kialakítandó adatvédelmi egyezmények gondolata már az évtized elején felmerült, felvetve egy egységes elveken alapuló európai szabályozás szükségességét, ahelyett, hogy azokat eltérő módon nemzeti szinteken szabályozták volna.

[6] A személyes adatok védelme kapcsán gyakran idézett példa a Schrems-ügy, amelyet egy osztrák állampolgár indított Facebook-adatainak Egyesült Államokban lévő szerverekre történő továbbítása kapcsán, hivatkozva arra, hogy – a 2013-ban kirobbant amerikai titkosszolgálati megfigyelési botrány információinak a fényében – adatai nincsenek biztonságban. Mivel az EUB „az olyan szabályozást, amely hatóságok számára lehetővé teszi, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához, a magánélet tiszteletben tartásához való, alapvető jogot sértőnek találta", így érvénytelenítette a határozatot. A példát lásd Európai Unió Alapjogi Ügynöksége – Európa Tanács: *Európai adatvédelmi jogi kézikönyv* 2018. évi kiadás, Luxembourg, Az Európai Unió Kiadóhivatala, 2019. 49.

[7] Európai Unió Alapjogi Ügynöksége – Európa Tanács (2019): i. m. 49.

Nemzetbiztonsági vonatkozásban az Európai Parlament LIBE Bizottsága[8] által az amerikai Nemzetbiztonsági Ügynökség (NSA) titkos adatgyűjtése és uniós állampolgárokat érintő tömeges elektronikus megfigyelése kapcsán 2013–2014 között lefolytatott vizsgálat[9] említendő, amelynek eredményeként még inkább hangsúlyossá vált az adatbiztonság és a személyes adatok védelme, mind a szabályzás szükségességének, mind a biztonság fokozására szolgáló technikai képességek megteremtése terén.

Széles körben terjedtek el a végpont–végpont közötti titkosítási megoldások, amelyek azonban a nemzetbiztonsági és egyéb bűnüldöző szervek számára is megnehezítették a szükséges információkhoz való hozzájutást. A titkosítások alkalmazásának sajátos paradoxona, hogy az egyre erősebb titkosítás nélkülözhetetlen a biztonság növelése érdekében akár az egyének szintjén, akár az állami rendszereknél, emellett azonban fontos azt is biztosítani, hogy az arra jogosult bűnüldözési, illetve nemzetbiztonsági szervek meghatározott feladataik mentén (például terrorizmus elleni küzdelem) hozzáférjenek a számukra szükséges és engedélyezett adatokhoz. A legismertebb, a médiában megjelent nemzetközi példaként a 2016-os FBI[10] vs. Apple[11] eljárás emelhető ki. Ennek során egy San Bernardinói terrorcselekményt követően az FBI bírósági eljárásban kérte az Apple közreműködését, egy, a rendszerében alkalmazott titkosítási funkció dekódolási módszerének általános átadására. A nemzetbiztonsági érdek versus személyes adatok precedensjellegű eljárás hatalmas nemzetközi visszhangot keltett, amely végén az FBI mégis külső közreműködéssel, egyedi hackereljárással szerezte meg az eszközről a kívánt adatokat.

Hasonló helyzetet láthatunk a Google-höz hasonló, az oroszországi internetes keresések túlnyomó részét uraló Yandex keresőszolgáltató elleni orosz állami fellépés esetében is. A korábban még együttműködőnek[12] tekintett szolgáltatót 2019-ben rendszerének állami blokkolásával fenyegették, mivel nem volt hajlandó átadni titkosítási kulcsait az orosz titkosszolgálatoknak, annak ellenére,

[8] Committee on Civil Liberties, Justice and Home Affairs – Állampolgári Jogi, Bel- és Igazságügyi Bizottság.

[9] Claude Moraes*: Working Document 1 on the US and EU Surveillance Programmes and Their Impact on EU Citizens Fundamental Rights.* Committee on Civil Liberties, Justice and Home Affairs, 2013.

[10] Federal Bureau of Investigation, Szövetségi Nyomozó Iroda.

[11] The Apple-F.B.I. Case. *The New York Times,* (2016).

[12] Ekaterina Drobinina: Russian Search-Engine Yandex Passed Information to FSB. *BBC News,* 2011. május 3.

hogy erre az orosz törvények kötelezték. A Yandex esetében ez szintén azt jelenthette volna, hogy állami oldalról általános lehetőség nyílna a személyes kommunikáció átfogó, rendszerszintű megfigyelésére. A kérést a szolgáltató már az internet szabadsága ellen vívott lépésként értékelte, és nem tett eleget az orosz titkosszolgálat kérésének.[13]

A legtöbb országban azonban a tiltás, korlátozás helyett, illetve mellett az állam önmaga is előszeretettel használja hivatalos információmegosztásra a globális infokommunikációs szereplők szolgáltatásait. Ilyenek a közösségi felületek, amelyek milliárdos felhasználói közössége lehetőséget nyújt az állami szféra számára az állampolgárok csoportos, de akár egyéni megszólítására is. Ma már általánosnak tekinthető, hogy a kor kihívásaira reagálva és a választók, állampolgárok széles körét elérve a politikusok a korábbi állami internetes oldalak mellett a nagyobb közösségi oldalakon (Facebook, Twitter) tesznek közzé hivatalos üzeneteket. Számos kutatás vizsgálta az amerikai elnökválasztások sorából Barack Obama korábbi amerikai elnök 2008-as választási kampányát, amely során már több mint 100 főt alkalmaztak digitális jelenlétének biztosítására, de ő használta először (a 2011-es előválasztások során) a YouTube-ot választási üzenetének közzétételére.[14] Donald Trump 2016-os választási kampányánál szintén jelentős szerepet kaptak a közösségi csatornák, ahol azonban már – mint arra a 2018-ban Facebook – Cambridge Analytica-botrány felhívta a figyelmet – a közösségi oldalakon keresztül történő célzott politikai befolyásolás és a személyes adatok helytelen kezelésének problémái is felszínre kerültek.[15]

Tiltás

Általánosan ismert Kína és a nagy keresőóriás Google viszonya, ahonnan a vállalat szolgáltatásával már tíz éve kivonult, mivel az állam a keresések cenzúrázását

[13] Fred Weir: Russian Internet Giant Yandex Takes Rare Stand Against State Snooping. *The Christian Science Monitor,* 2019. június 14.

[14] Contentgroup: Social media on the campaign trail: Barack Obama and Donald Trump. (2017).

[15] Az évekig húzódó (2015–2019) Cambridge Analytica adatelemző cég botránya, amely során 87 millió amerikai Facebook-profilját használta fel egy profilozásra, elemzésre alkalmas szoftver létrehozásához, amely eredményeként például személyre szabott politikai hirdetésekkel befolyásolni lehetett amerikai szavazókat a 2016-os amerikai elnökválasztási kampány alatt. Lásd Kurt Wagner: Facebook Says Cambridge Analytica may have had Data from as Many as 87 Million People. *Vox,* 2018. április 4.

várta el. A piaci érdekek mentén igaz, az elmúlt években ismét felmerült a kínai állam számára hozzáférést biztosító keresőmotor *(Dragonfly)* fejlesztésével a piacra történő visszatérése, hiszen így egy több mint egymilliárdos ország piaci szegmense maradt meg a kínai IKT-szektor számára. Oroszországban hasonló piaci és a nemzetbiztonsági érdekek találkozását láthatjuk. 2019-ben a hatóságok felszólították a Google-t, hogy állítsák le a cég tulajdonában lévő YouTube-on közzétett és „Oroszországban törvényellenesnek minősített tömegmegmozdulások hirdetését", és felmerült a keresőmotor elérésének blokkolása is. Ugyanakkor az Apple – vélhetően szintén piaci megfontolások miatt – lépéseket tett arra, hogy a nemzeti szintű elvárásoknak megfelelve Kína, valamint Oroszország esetében is biztosítsa, hogy az adott országok határain belül tárolja a honos állampolgárok adatait.[16] Oroszország esetében terrorizmusellenes törvény (Jarovaja tv.) alapján így együttműködési kötelezettsége jelenik meg a biztonsági szolgálatok irányába is.

A kommunikáció szabadsága és az állami szintű megfigyelési lehetőségek körüli vitákhoz sorolható az orosz VKontakt közösségi oldal korábbi példája, amely sikertelenül próbált meg ellenállni az orosz állami elvárásoknak, vagy akár a blokkolással fenyegetett Telegram üzenetküldő elterjedt alkalmazása, amely titkosítást alkalmazva biztosítana védelmet felhasználói kommunikációja számára.[17]

Idesorolhatók azon gyakorlatok is, amikor egyes államok a nemzeti szintű biztonsági érdekeik kapcsán bizonyos infokommunikációs területeken a függetlenségre való törekvés útját választják. A kiberbiztonság szempontjait tekintve ezek főként az államigazgatás területén figyelhetők meg, így például saját hírközlési és adatátviteli rendszerek, illetve zárt kommunikációs szolgáltatások kiépítése és az azokra való áttérés (nemzeti szintű mobiltelefon- vagy akár levelezési szolgáltatások kialakítása). Franciaországban például a külföldi titkosszolgálati megfigyeléseket elkerülendő a BlackBerry okostelefon internetezésre való tiltása az államigazgatásban már 2007-ben megjelent, de a 2013-as amerikai titkosszolgálati botrány után a francia kormányzat érzékeny területein az általánosan használt mobiltelefonok helyett a francia Thales hadiipari cég mobiltelefonjának (Teorem) használatát írták elő.[18] Az amerikai haditengerészet pedig 2019 végén a rendkívül gyors ütemben terjedő (a kínai ByteDance tulajdonában álló) TikTok

[16] Amy Mackinnon: How Russia is Strong-Arming Apple. *Foreign Policy,* 2019. január 31.
[17] Domokos Erika: Oroszország letilt egy üzenetküldő szolgáltatást. *Napi.hu,* 2018. április 13.
[18] MTI: Hadat üzent a Gmail-nek a francia kormány. *Napi.hu,* 2013. szeptember 13.

mint közösségimédia-alkalmazás letöltését és használatát tiltotta be kiberbiztonsági okokból a kormány által biztosított okostelefonokon és táblagépeken.[19]

A kínai példa

A kínai példa annak sajátosságai és a megfigyelés általános jellege miatt mindenképpen áttekintésre érdemes. Kína napjainkra széles körű megfigyelési technológiai eszközrendszereket épített ki az országban, amelyek szintje a világon addig sehol nem látott méreteket öltött, és amely fejlett technológiákkal rendkívül széles körben (az emberek mozgásától kezdve egyéb elektronikus kommunikációjukig) megfigyelhetik tevékenységüket. Nemzetközi szakirodalmi források több mint 200 millió biztonsági kamerát említenek, amely szám 2022-re várhatóan 213%-kal, 626 millióra fog emelkedni. Ezek egyéb IKT-megoldásokkal, arcfelismeréssel, az egyén mozgásának nyomon követésével, egyéb adatbázisokban tárolt személyes adatokkal történő összevetésével és a mesterségesintelligencia-alkalmazásokkal együtt már a társadalom mindennapjainak átfogó elemzését biztosíthatják, elősegítve a kínai „társadalmi érdemeken alapuló kívánt viselkedés elfogadását ösztönző" társadalmi pontrendszer bevezetését.[20]

A kínai „megfigyelési technológia" exportja a 2008-as pekingi olimpia után kezdődött, amely óta Kína 54 országba exportálta a magánéletre hatást gyakorló megfigyelőrendszereit.[21] Míg a szakirodalmi források alapvetően a „tekintélyelvű" kormányok működéséhez kapcsolják a széles körű, a társadalom tagjait érintő megfigyelési alkalmazásokat, mindezek egy-egy kiemelt biztonsági kihívás kapcsán (például terrorizmus, bűncselekmények, sportrendezvények) jelen vannak a világ demokratikus állami berendezkedésű régióiban, nagyvárosaiban is (például London). E képességek az „okos város" technológiái mentén is várhatóan megjelennek, így kiemelten fontossá válik az adatok tárolásának és felhasználhatósága szabályozásának változó technológiai környezethez történő igazítása.

[19] Dalvin Brown: The U.S. Navy Banned TikTok from Government-Issued Smartphones over Cybersecurity Concerns. *USA Today,* 2019. december 23.

[20] Tenzin Dalha: Beijing's Export of Surveillance Technology. *Modern Diplomacy,* 2020. január 7.

[21] Dalha (2020): i. m.

Dobák Imre

A kutatás, fejlesztés és innováció átrendeződése nemzetbiztonsági szemmel

A 21. századi nemzetbiztonsági struktúrák – amelyekkel szemben társadalmi és „szakmai" elvárás, hogy korszerű megoldásokkal, rendkívül képzett állománnyal és megfelelő reagálási lehetőségekkel rendelkezzenek – eszközei, megoldásai, személyi utánpótlásuk jelentős része is ebben a „megoszthatatlan" környezetben fejlődnek. Más ágazatoktól eltérően céljaikat nem a profitorientáltság, hanem az állam biztonsági igényeinek kielégítéséhez való hozzájárulás, az abban történő részvétel határozza meg.

A múlt század keleti–nyugati szembenállásának időszakában a különböző technológiák fejlesztésénél és felhasználásánál az egyes államok törekedtek a nemzeti, illetve szövetségesnek tekintett országok különböző szektoraiban létrehozott technikai megoldások alkalmazására, így széles kapcsolatokat építettek ki a külső, tudományos kutatóintézeti és együttműködő vállalati környezet irányába. Ennek az időszaknak a fejlesztési sajátosságaira többek között az alábbiak voltak jellemzők:

- a hidegháborús szembenálláshoz igazodó rendkívüli technológiai verseny;
- a technikai rendszerek létrehozása történelmileg vagy az állami oldalon történt, vagy azok fejlesztése, beszerzése sajátos zárt kapcsolatot igényelt a nemzeti iparral, amelyet a titoktartás jellemzett;
- az ipari, technológiai, gazdasági jellegű hírszerzés kiemelt jelentősége;
- a nemzeti szinteken rendelkezésre álló K+F képességek és kapacitások felhasználása, a nemzeti szintű (állami) „külső" kutatóintézetek, egyetemek nem nyilvános módon történő bevonása;
- a szövetségesi rendszerben partnerként megjelenő országokkal való technikai, technológiai, tudományos együttműködések és tapasztalatcserék.

Globális információs társadalmunkban mindennek szempontjai azonban átalakultak. Napjainkban a technológiai fejlesztések és a K+F eredmények túlnyomó része már az állami szférán kívül, a piaci, vállalati szférában keletkezik, és számos területen a korábbi elzártság már nem megvalósítható. Ennek okai között jelennek meg, hogy a 21. századi korszerű elektronikus információmegosztási formák, a tudomány új eredményeihez való globális hozzáférés, a fejlesztési képességek és központok decentralizálódása, valamint az internetre és az informatikára épülő szabad fejlesztési lehetőségek rendkívüli módon átalakították

a kutatás-fejlesztés és innováció (K+F+I) rendszerét, amely napjainkra a fejlődés egyik legmeghatározóbb területévé vált.

Amíg az új technológiák előnyei egyértelműnek tűnnek, addig nemzetbiztonsági szempontból azok megjelenése kapcsán gondoljunk egyszerűen a magánszférában vagy akár másik országban fejlesztett olyan megoldásokra, amelyek (állami szférába történő) beáramlása azonban kockázatokat is rejthet magában.[22] A Kadtke–Warton szerzőpáros a technológiai nagyhatalom Egyesült Államok esetében fogalmazza meg, hogy „számos tényező miatt az új technológiák következő generációja valószínűleg az Egyesült Államokon kívül kerül forgalomba és gyártásra, ami stratégiai és hosszú távú veszélyt jelent".[23]

Minderre talán a legjobb példa, a világunkra mindenképpen hatást gyakorló 5G technológia bevezetése,[24] amely már önmagában is – mint az egyes nemzeteken túlmutató és globális vállalati szereplők részvételével zajló – technológiai rivalizálás színtere. A hagyományosnak tekinthető kommunikációs megoldásokkal szemben szakértők hívják fel a figyelmet arra, hogy az 5G kiépülése várhatóan alapjaiban fogja megváltoztatni társadalmunk számos szegmensét. Eszközök tömegei fognak valós időben kommunikálni egymással és az IoT- (*Internet of Things,* dolgok internete) megoldások, az internetre csatlakozó szenzorok milliói várhatóan életünk több területét is a technikai adatok által vezérelt irányba mozdítják el. Tovább fejlődnek a tömeges adatok feldolgozásának újszerű megoldásai, és ezzel párhuzamosan a mesterséges intelligencia alkalmazásai.[25]

Az 5G politikai jelentősége is vitathatatlan, gondoljunk csak a technológiai élmezőnybe tartozás gazdasági, társadalomfejlődési és biztonsági hatásaira. Számos ország (például Kína, Dél-Korea, Japán és több EU-tagország) már kijelölte a rendszer működéséhez szükséges frekvenciaspektrumot, és jelenleg már a hálózatok kiépítése, a regionális szolgáltatásindítás, valamint az infra-

[22] A piaci, nemzetgazdasági, valamint nemzetbiztonsági kérdéskörök találkozásánál számos olyan nemzetközi példa látható, amelyek jól jelzik ezen kérdéskörök összetettségét. 2018-tól zajló gazdasági háborúvá növekvő folyamat része a kínai Huawei mobilkommunikációs óriáscég nemzetbiztonsági kockázatra való hivatkozással, Egyesült Államokból történő kitiltásának kérdése.

[23] James Kadtke – John Wharton: Technology and National Security: The United States at a Critical Crossroads. *Defense Horizons,* 2018. március 1.

[24] Az 5G-szabvány végleges változatának jóváhagyását 2020 elejére tervezte a Nemzetközi Távközlési Unió (ITU).

[25] Andrej Kadomtsev: 5G: A new stage in civilization development amid global competition. *Modern Diplomacy,* 2019. december 26.

struktúra technológiai – gazdasági szempontrendszerei körül folynak a gyakran „gazdasági csatározásokba" torkolló nemzetközi viták.[26]

A kérdéskör összetettségét, jövőbe mutató gazdasági és nem utolsósorban társadalmi súlyát jelzik az egyes országok eltérő álláspontjai is. Míg Kína ellenőrzi a „világ 5G-szabadalmainak több mint egyharmadát, és a meglehetősen korlátozott számú potenciális fejlesztői és gyártói kört",[27] az európai országok többsége támogatja annak bevezetését, az Egyesült Államok esetében pedig a kínai technológiai kiszolgáltatottságtól tartva, a technológiai lemaradás behozatalához való időnyerés vagy akár egy későbbi technológiai piaci pozíciószerzés előkészítése sejthető.

A technológiai-gazdasági fölényért vívott küzdelemben kiemelten fontos nemzetbiztonsági kérdésként merül fel, hogy lehet-e, és ha igen, milyen mértékben egy adott társadalom működését alapjaiban meghatározó technológiai infrastruktúrát, a felhasználók életének szinte minden területére kiterjedő adatokat egy másik országnak vagy akár multinacionális nagyvállalati szereplőnek kiszolgáltatni. Mennyiben veszélyeztetheti ez az adott nemzet és a társadalom szuverenitását, vagy pedig ennek ellenoldalaként a korszerű megoldások hiányában a technológiai elszigetelődés és a gazdasági-társadalmi lemaradás veszélye fenyegethet. A jövőben minden bizonnyal egyre gyakrabban találkozunk majd az új technológia biztonságra gyakorolt kérdései körül felmerülő dilemmákkal.

Anélkül, hogy a biztonságra, védelemre és a hadviselésre a jövőben hatást gyakorló egyéb technológiákat felsorolnánk jelen fejezetben, megállapítható, hogy egyre fontosabbá válik a különböző technológiák folyamatos monitorozása, és annak megállapítása, hogy azok a jövőben kulcsfontosságúnak tekinthetők-e, hogyan befolyásolják egy adott nemzet védelmi képességeit, biztonsága növelésének lehetőségeit, valamint a nemzeti ipar szintjén rendelkezésre állnak-e annak fejlesztési képességei.[28]

[26] Lásd: az Egyesült Államok és Kína között kirobbant gazdasági háború, a kínai Huawei cég térhódítása.

[27] Kadomtsev (2019): i. m.

[28] Quentin Ladetto: *Defence Future Technologies, Emerging Technology Trends 2015.* (DEFTECH) Federal Department of Defence, Civil Protection and Sport DDPS Armasuisse Science and Technology, 2016.

Nemzetbiztonság és a kiszervezés

A nemzetbiztonsági rendszer működésének sajátosságai, annak központi és kritikus elemei, valamint a döntéseket segítő feladatrendszere miatt általánosságban megfogalmazható, hogy annak ellátása elválaszthatatlan állami feladat. Mint Finszter Géza is kifejti tanulmányában:

> „A nemzetbiztonság nem privatizálható. Ennek oka egyfelől a fenyegetések súlyosságában, másfelől az elhárításukra alkalmas eszközök jogkorlátozó természetében található. Ezek együtt államigazgatási felhatalmazást és felelősséget igényelnek. Alkotmányos rendszerekben ez a sajátos erőszak-monopólium is a jog uralma alatt áll, és gyakorlása nem korlátlan."[29]

Fentiek ellenére a nemzetbiztonság és az üzleti alapon működő magánszektor témakörét vizsgálva, bizonyos területeken mégis találkozhatunk az úgynevezett *outsourcing,* vagyis adott feladatok üzleti alapon történő kiszervezésének gyakorlatával. A jelenség kapcsán a nemzetközi szakirodalmak is alapvetően annak alkotmányossági problémájára hívják fel a figyelmet, annak az elvi kérdésére, hogy – akár az ellenőrzési funkció megtartásával is – az állam „erőszak-monopóliumához" tartozó tevékenységek kiadhatók-e egyáltalán külső együttműködő partner számára?

A biztonságért felelős ágazatok szélesebb körét tekintve a kiszervezés általánosan elfogadott jelenség, gondoljunk csak a rendészeti tevékenység bizonyos területeire (például őrző-védő cégek), hiszen „a közbiztonság nem csupán állami szolgáltatás, hanem megvásárolható áru".[30] Mindezt erősíti, hogy a biztonság olyan közös társadalmi érdek, ahol a feladatok nemcsak adott állami szervek, hanem a magánszféra és az egyének közös munkáját is szükségessé tehetik, ezzel azonban sajátos piaci lehetőségek jönnek létre. Mint Balogh László Levente megfogalmazza tanulmányában, az erőszak-privatizáció „egy egyre dinamikusabban fejlődő erőszakpiac kialakulását, és az erőszak bizonyos formáinak magánkézben való összpontosulását jelenti".[31] Az erőszak-privatizáció folyamatának irányai kapcsán, tanulmányában[32] alulról felfelé irányuló *(bottom-up),* és felülről lefelé irányuló *(top-down)* formákat különböztet meg, ahol formai értelemben

[29] Finszter (2019): i. m. 105.
[30] Finszter (2019): i. m. 101.
[31] Balogh László Levente: Állam és erőszak. *Politikatudományi Szemle,* 20. (2011), 1. 119–132.
[32] Balogh (2011): i. m. 130.

a „felülről lefelé irányuló" formához – ahol a gazdasági kiadások csökkentése és a hatékonyság növelésének egyéb indokai kereshetők – sorolja a biztonsági szektor önálló gazdasági ágazattá válását. Ennek értelmében a nemzetbiztonság egyes elemei is ehhez a formához sorolhatók, bár azon véleményeknek is helye lehet, hogy a rendkívül érzékeny nemzetbiztonság semmilyen területen nem szervezhető ki.

A gyakorlatban, napjaink összetett feladatrendszerei alapján a pontos választóvonal rendkívül nehezen határozható meg, ugyanakkor a nemzetközi példák kapcsán az is látható, hogy a hatékonyság növelése érdekében a nemzetbiztonsági szféra is gyakran fordul a számára megbízhatónak vélt külső vállalati feleknél meglévő képességek felé. Ez az együttműködés azonban még nem feltétlen jelenti az adott tevékenység kiszervezését, gyakran csak a nemzetbiztonsági célú feladatok, illetve az információgyűjtést segítő folyamatok elengedhetetlen, illetve azt hatékonyan támogatni tudó nemzetbiztonsági kapcsolatrendszereinek működtetését jelentik. Látható, hogy vannak olyan területek (például fejlesztési, informatikai, logisztikai, képzési területek adott részei), amelyek bizonyos elemeiben akár leválaszthatók is lehetnek a nemzetbiztonsági feladatkör központi elemétől, és amelyekre a struktúra, hasonlóan más állami szervekhez, egyszerűen piaci megrendelőként tekinthet. Az ezeken a területeken igénybe vett szolgáltatás/termék alapvetően nem különbözik egy civil szereplőnek nyújtottól, ráadásul e képesség kiépítése, fenntartása akár rendkívüli erőfeszítéseket is okozhat az adott szervezet számára (gondoljunk csak a piaci alapon működő informatikai fejlesztésekre, amelyekre az amerikai titkosszolgálati botrány is ráirányította a figyelmet).

Az együttműködés két fő formáját tekintve (lásd Pap András László munkájában[33] „diszpozitív" és „kógens" típusok), megjelennek a jogszabályi kötelezettségen alapuló együttműködési formák, illetve az adott fél önkéntes (alapvetően piaci alapú) együttműködésének lehetősége. Az első esetben gondolhatunk például a pénzintézeteket, postai vagy akár infokommunikációs szolgáltatókat együttműködésre kötelező jogszabályokra. A második (piaci alapon kialakuló együttműködési) forma kapcsán az adatfeldolgozás vagy akár a kutatás-fejlesztés területén megvalósuló együttműködések, kutatási célú kapcsolatok említhetők. E kapcsolatoknak létezhet egy, a partnerség jegyeit mutató (közös munkán és érdekeltségen alapuló) formája és egy mélyebb, az egész

[33] Pap András László: *A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig.* Budapest, L'Harmattan, 2012. 40–41.

tevékenységet kiszervező formája. Adott területeken megtalálható az úgynevezett PPP *(Public-Private Partnership)* a köz- és magánszféra közötti partnerségi típus is, amely alkalmazásának megítélése szintén vitatottnak tekinthető, hiszen akár ütköző érdekek, így a „biztonsági ügynökségek biztonságot maximalizáló logikája és a magánvállalatok profitmaximalizáló logikája”[34] találkozhat. Az aggodalmak kapcsán a magánszektor szereplőinek „elszámoltathatósága, felügyelete és legitimitása” is felmerülhet.[35]

Tényként állapítható meg, hogy a különböző szintű együttműködések jelentősége napjainkban egyre inkább felértékelődik, hiszen a nemzetbiztonsági szervezetek sem tudják leválasztani tevékenységüket, képességeik fejlesztését a külső, rendkívüli ütemben fejlődő környezettől. Idesorolhatók a titkosszolgálati technológiák „kereskedelmi piacán” megjelenő vállalkozásokkal fenntartott, eszközrendszerek beszerzésére, akár a sajátos tudásbázist igénylő szoftverek és megoldások fejlesztésére irányuló együttműködések. Jelen vannak a nagy mennyiségű adatok feldolgozására szakosodott privát cégek, amelyek például az internet és a közösségi felületekhez kapcsolódó fejlesztéseikkel, termékeikkel kínálhatnak egyedi megoldásokat felhasználóik számára (például kémszoftverek alkalmazása). Itt értelmezhetők a nyílt forrású információgyűjtés (OSINT) üzleti alapon működő célirányos termékei, amelyeket mind az állami, mind a piaci szektor előszeretettel alkalmaz, vagy akár az úgynevezett adatbróker cégek, amelyek a különböző helyeken keletkező adatok megszerzésével, akár azok elemzésével-értékelésével kapcsolódhatnak a biztonsági szervek munkájához. Ennek gyakorlatát főként az amúgy is elterjedt nemzetbiztonsági kiszervezési megoldásokkal érintett országokban (például Amerikai Egyesült Államok) láthatjuk.

Habár a piaci alapon működő együttműködés formáihoz sorolható, mégis talán attól elkülönülten érdemes megemlíteni a nemzetbiztonságot közvetlenül befolyásoló fegyveres konfliktusokban a hírszerzéssel-felderítéssel, őrzéssel-védelemmel, logisztikai feladatokkal foglalkozó magáncégek, katonai magánvállalatok igénybevételének rendkívül vitatott, sokszor botrányoktól kísért nemzetközi példáit. Alkalmazásuk során gyakran az állami és gazdasági szereplők egybeeső kormányzati és üzleti érdekei (például olajipari érdekeltségek védelme a konfliktustérségben) és nem utolsósorban szerződéses viszonyuk (így elszámoltathatóságuk korlátja)

[34] Oldrich Bures – Helena Carrapico: Private Security beyond Private Military and Security Companies: Exploring Diversity within Private-Public Collaborations and its Consequences for Security Governance. *Crime, Law and Social Change,* 67, (2017), 3. 229–243.

[35] Bures–Carrapico (2017): i. m. 237.

jelenik meg. Alkalmazásukra és azok mértékére számos nemzetközi példát láthatunk,[36] jelentősége a hibrid hadviselés kapcsán vélhetően a későbbiekben is erősödni fog.

Nemzetbiztonsági értelemben sajátos állami és vállalati együttműködésként jelentkezik a fedőtevékenységre használt üzleti-gazdasági környezet kialakítása, illetve nemzetbiztonsági feladatokba történő bevonása. Ugyanakkor ezek nem sorolhatók a hagyományos értelemben vett kiszervezés kategóriájához, hiszen mögöttük valójában nemzetbiztonsági szervek állnak, és a működtetés okait, formáját is a nemzetbiztonsági érdekek mentén kell keresnünk. A szolgálatok számára feladatként, a civil piaci szereplőkkel azonos gazdasági környezetben működő, azonban ellenérdekelt nemzetbiztonsági kötődésű vállalatok kiszűrése jelentheti, hiszen a velük való esetleges együttműködés már biztonsági kockázatot hordozhat magában. 2020 elején került nyilvánosságra, hogy a semlegesség szimbólumaként megjelenő Svájcban, a világ egyik vezető rejtjelező eszközök gyártásával foglalkozó vállalata (Crypto AG.) 2018-ig, közel 50 éven keresztül az Egyesült Államok hírszerzésének (CIA) a tulajdonában volt.[37] A külföldi kormányoknak rejtjelező eszközöket biztosító vállalaton keresztül így az amerikai fél számára hozzáférés nyílhatott mások féltve őrzött titkaihoz. A megoldás – ha talán nem is ilyen eredményességgel – jelen lehet más országok gyakorlatában is, így biztonsági szempontból a nemzetbiztonsági ágazatban általánosságban a nemzeti, állami vállalatokkal való együttműködést preferálják.

Összességében a kiszervezés tevékenysége kapcsán számos olyan kérdés merülhet fel, amelyek befolyásolhatják a nemzetbiztonsági gondolkodás és felhasználás jövőbeli alakulását. Ezek között vethetők fel az alábbi teoretikus kérdések:

– Melyek azok a szolgálatok működéséhez kapcsolódó területek, amelyek a „nemzetbiztonság" sérelme nélkül kiszervezhetők egy piaci alapú környezetbe, és milyen mértékben? (Itt érdemes hangsúlyozni, hogy egy

[36] Az Amerikai Egyesült Államok példáját kiemelve, a katonai magánvállalatok és magán hírszerző cégek alkalmazása nem történeti előzmények nélkül való. A II. világháború időszakában a hírszerzés és információgyűjtés területén például a Pond (1942–1955) [lásd Mark Stout: The Pond: Running Agents for State, War, and the CIA. The Hazards of Private Spy Operations. Studies in Intelligence, 48. (2004), 3. 69–82.] nevű szervezet vált ismertté, majd 50 évvel később az Eric Prince által alapított, külföldi katonai konfliktusokban sajátos szerepet betöltő Blackwater szervezete került vitatott tevékenységével a nyilvánosság középpontjába.

[37] Imogen Foulkes: Swiss Crypto AG spying scandal shakes reputation for neutrality. *BBC News,* 2020. február 16.

adott terület teljes kiszervezése a képességvesztés elkerülése érdekében akár kényszerű folyamatos együttműködésre ítélheti a szervezeteket.)
- Milyen formáló (káros vissza)hatása lehet a kiszervezésnek (például fejlesztés) a nemzetbiztonság központi folyamataira?
- Mennyire tekinthető megbízhatónak az adott együttműködő fél által biztosított információ (adatbrókerek jelenléte), és ez torzíthatja-e a nemzetbiztonsági szolgálat döntés-előkészítési tevékenységét?
- Mennyire és hogyan biztosítható a nemzetbiztonsági és információgyűjtési érdekek hosszú távú védelme?
- A korábban szervezeten belül végzett folyamatok külső együttműködő környezetbe helyezése hogyan befolyásolhatja az állomány elvándorlását? (Különösen érintett az IT-szektor, ahol a magasabb fizetések hatása nemzetközi példák alapján is jól látható.)[38]

A nemzetközi szakirodalom alapján elmondható, hogy az ezredfordulót követően a terrorizmus elleni küzdelem felerősödésével a kiszervezés súlya felerősödött, bár a 2013-ban kirobbant amerikai megfigyelési botrány rávilágított a megoldás sérülékenységére is. Amellett, hogy a gyakorlat segítheti adott területeken a gazdaságosabb működést, akár a külső környezethez igazodó innovatív ismeretek becsatornázását, számos biztonsági kockázatot hordoz magában. Sérülhet a nemzetbiztonsági tevékenységek irányainak, képességeinek titkossága, de a profitorientált üzleti szemlélet torzíthatja is a nemzetbiztonsági feladatok ellátását. Az érintett piaci szereplők egy idő után a nyereségük növelése érdekében a folyamatokat befolyásoló politikai szereplők számukra kedvező döntése érdekében lobbitevékenységeket kezdhetnek.[39] Rendkívül szélsőséges esetben egyes döntések is piacorientálttá válhatnak, „miközben az állam egyedülálló legitimációjának köszönhetően a politikai döntések sohasem követhetik kizárólag a magánhaszon elveit".[40]

[38] Adott feladatok (például K+F) kiszervezése esetén gyakran a korábban állami szférában dolgozó alkalmazottak már a profitorientált vállalati környezetben, sajátos jogviszonyban (például szerződéssel) végzik el a korábban még az állami szférában teljesített feladatokat.

[39] A biztonság szélesebb területei kapcsán lásd Bures–Carrapico (2017): i. m. 239.

[40] Balogh (2011): i. m. 131.